In the Claims:

Claims 1-44 (Canceled)

45. (New) Hardware unit for controlling access, by a processor to a peripheral (P) of this processor, said hardware unit including:

means of triggering an interrupt of said processor, termed a control interrupt;

means of obtaining, from said processor and after said triggering, an access authorisation code (Code-AA) to said peripheral (P);

internal means of comparing said access authorisation code (Code-AA) with a predetermined reference value (Code-UMCA); and

so-called validation means designed to generate an electrical signal (SIG_VAL) to validate an access electrical signal (CS, WE, PWR) to said peripheral (P), depending on the outcome of said comparison, wherein said hardware unit is external to processor and in that it includes means of generating said reference value (Code-UMCA) according to a predetermined law.

46. (New) Access control hardware unit according to claim 45, wherein said control interrupt is a non-maskable interrupt (NMI1).

47. (New) Control hardware unit according to claim 45, wherein it additionally includes means of obtaining a trigger code (Code-DD), and in that said means of triggering said

control interrupt (NMI1) are designed to trigger said interrupt following the acquisition of said trigger code (Code-DD).

48. (New) Access control hardware unit according to claim 47, wherein it additionally includes means of comparing said trigger code (Code-DD) with said predetermined reference value (Code-UMCA), and in that said triggering means are designed to trigger said control interrupt (NMI1) depending on the outcome of said comparison.

49. (New) Access control hardware unit according to claim 45, wherein it includes means of triggering an interrupt of said processor, termed an alarm interrupt, when said access authorisation code (Code-AA) or said trigger code (Code-DD) is different from the predetermined reference value (Code-UMCA).

50. (New) Access control hardware unit according to claim 49, wherein said alarm interrupt is a non-maskable interrupt (NMI2).

51. (New) Access control hardware unit according to claim 45, wherein said predetermined reference value (Code-UMCA) is a counter initialised when said hardware unit is switched on (UMCA), and in that, according to said predetermined law, said counter is incremented each time said access authorisation code (Code-AA) is obtained.

52. (New) Access control hardware unit according to claim 45, wherein said validation means include logic combination means designed to:

receive an electrical signal requesting access (CS-RQ, WE-RQ) to said peripheral (P);

receive said validation signal (SIG_VAL); and

validate said access electrical signal (CS, WE) as a function of a state (RQ_0, RQ_1) of said access request electrical signal (CS-RQ, WE-RQ), a state (VAL_0, VAL_1) of said validation signal, and a logic represented in a truth table.

53. (New) Access control hardware unit according to claim 52, comprising means of reading a state (RQ_0, RQ_1) of said access request electrical signal (CS_RQ, WE_RQ), and means of triggering an interrupt of said processor, termed an alarm interrupt (NMI2), preferably non-maskable, as a function of this state (RQ_0, RQ_1) and of said state (VAL_0, VAL_1) of said access validation electrical signal (SIG_VAL).

54. (New) Access control hardware unit according to claim 45, wherein it includes means of inhibiting said validation signal (SIG_VAL).

55. (New) Access control hardware unit according to claim 54, wherein said inhibiting means are designed to inhibit said validation signal (SIG_VAL) following at least one access to said peripheral (P).

56. (New) Access control hardware unit according to claim 54, wherein said inhibiting means are designed to inhibit said validation signal (SIG_VAL) after a predetermined delay counted from the generation of said access validation electrical signal (SIG_VAL), or from the acquisition of said access code (Code-AA).

57. (New) Method of controlling access, by a processor to a peripheral (P) of this processor, wherein it includes the following steps:

triggering (E34) an interrupt of said processor, termed control interrupt;

obtaining (E37), from said processor and after said triggering, an access authorisation code (Code-AA) to said peripheral (P);

comparing (E38) said access authorisation code (Code-AA) with a predetermined reference value (Code-UMCA);

generating (E50) an electrical signal (SIG_VAL) validating an access signal (CS, WE, PWR) to said peripheral (P), depending on the outcome of said comparison step (E30), wherein said method is adapted to be executed by an hardware unit (20) according to claim 45, external to said processor and in that it additionally includes a step (E40) of generating said reference value (Code-UMCA) according to a predetermined law.

58. (New) Access control method according to claim 57, wherein said control interrupt is a non-maskable interrupt (NMI1).

59. (New) Access control method according to claim 57, wherein said triggering step (E34) is performed after a step of obtaining (E25) a trigger code (Code-DD).

60. (New) Access control method according to claim 59, wherein it additionally includes a step (E30) of comparing the trigger code (Code-DD) with said predetermined reference value (Code-UMCA), and in that said triggering step (E34) is performed depending on the outcome of said comparison step (E30).

61. (New) Access control method according to claim 57, wherein it includes a step (E100) of triggering an interrupt of said processor, termed an alarm interrupt, when said access authorisation code (Code-AA) or said trigger code (Code-DD) is different from the predetermined reference value (Code-UMCA).

62. (New) Access control method according to claim 61, wherein said alarm interrupt is a non-maskable interrupt (NMI2).

63. (New) Access control method according to claim 57, wherein said predetermined reference value (Code-UMCA) being a counter, it additionally includes a step (E10) of initialising said counter, said counter being incremented during said generation step (E40).

64. (New) Access control method according to claim 57, wherein during said step (E50) of generating the validation signal:

the state (RQ_0, RQ_1) of an electrical signal (CS-RQ, WE-RQ) requesting access to said peripheral (P) is read;

the state (VAL_0, VAL_1) of said validation signal (SIG_VAL) is read; and

said access electrical signal (CS, WE) is validated as a function of said state (RQ_1) of said access request electrical signal (CS_RQ, WE_RQ), of said state (VAL_1) of the validation signal (SIG_VAL), and as a function of a logic rule.

65. (New) Access control method according to claim 64, wherein it includes a step (E20, E36) of reading a state (RQ_0, RQ_1) of said access request electrical signal (CS_RQ, WE_RQ), and a step (E100) of triggering a maskable interrupt of said processor, termed an alarm interrupt, preferably non-maskable (NMI2), as a function of said state (RQ_0, RQ_1) and of said state (VAL_0, VAL_1) of said access validation electrical signal (SIG_VAL).

66. (New) Access control method according to claim 57, wherein it includes a step (E70) of inhibiting said validation signal (SIG_VAL).

67. (New) Access control method according to claim 66, wherein said inhibiting step (E70) is performed following at least one step (E65) of accessing said peripheral (P).

68. (New) Access control method according to claim 66, wherein said inhibiting step is performed after a predetermined delay counted from said step (E50) of generating the validation signal (SIG_VAL) or from the step (E25) of obtaining said trigger code (Code-DD).

69. (New) Method of managing access to a peripheral (P), wherein it includes a step of implementing a routine (IRT1) associated with a control interrupt, preferably non-maskable (NMI1), said control routine including :

a step (E510) of generating, according to a predetermined law, an access authorisation code (Code-AA) to said peripheral (P) ; and

a step (E520) of sending an access authorisation code (Code-AA) to an access control hardware unit according to claim 45.

70. (New) Method of managing access according to claim 69, wherein said access authorisation code (Code-AA) being a counter, it additionally includes a step of initialising said counter (Code-AA), and in that said generation step (E510) consists in incrementing said counter (Code-AA) before each sending (S100) of this code (Code-AA) to said hardware unit.

71. (New) Method of managing access according to claim 69, wherein it additionally includes a step of implementing an alarm interrupt routine (IRT2), said alarm routine including a step of generating an alert and/or inhibiting the use of said peripheral.

72. (New) Computer program including an instruction (E630) to access a peripheral (P), wherein it includes an instruction (E620) to send a trigger code (Code-DD) to an access control hardware unit of said peripheral (P) according to claim 45, before the execution of said access instruction.

73. (New) Computer program according to claim 72, wherein it additionally includes means of generating said trigger code (Code-DD) according to said predetermined law.

74. (New) Processor designed to implement a method of managing access according to claim 69.

75. (New) Use of an access control hardware unit (20) according to claim 45, to validate an access signal to a peripheral (P) which can in particular be selected from a screen, a keyboard, a memory, a communications interface controller, a memory management unit (MMU) or a memory protection unit (MPU).

76. (New) Processor designed to implement a computer program 72 according to claim 72.